(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 March 2002 (14.03.2002)

PCT

(10) International Publication Number
WO 02/21799 A1

(51) International Patent Classification[7]: H04L 29/06, G06F 17/00, H04L 9/32

(21) International Application Number: PCT/SE01/01901

(22) International Filing Date:
6 September 2001 (06.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0003171-6 7 September 2000 (07.09.2000) SE

(71) Applicant *(for all designated States except US)*: **BANK-GIROCENTRALEN BGC AB** [SE/SE]; S-105 19 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LANDBERG, Karl, Erik** [SE/SE]; Storängsstigen 1, S-182 74 Stocksund (SE). **BERGLUND, Anna, Elisabeth** [SE/SE]; Karlavägen 21, S-181 32 Lidingö (SE).

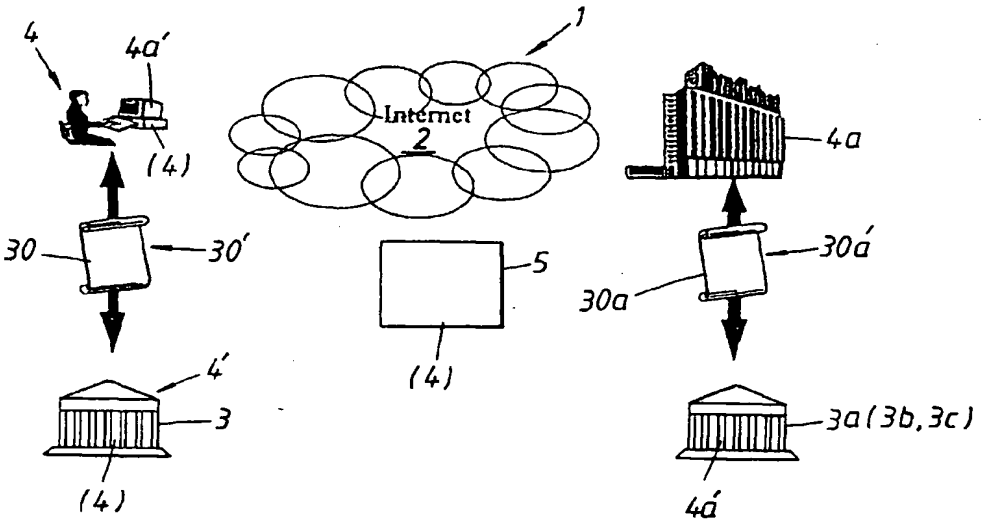
(74) Agents: **KARLSSON, Leif** et al.; L.A. Groth & Co. KB, Box 6107, S-102 32 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: NETWORK RELATED IDENTIFICATION SYSTEM



(57) Abstract: A network-related user identification system (1) in which a number of actors (3, 3a) at least two actors, are connected to the network (2), in which a plurality of users (4, 4a) are connected to the network (2), in which the actors (3, 3a) and the users (4, 4a) communicate with each other via said network, and in which one or more users (4) is/are identified (4') by at least one actor, a first actor (3), via an established procedure chosen by the actor or corresponding entity. The first actor (3) is able to allocate to a user (4) identified (4') by said first actor an ID-certificate (4) that is valid in respect of several actors (3a, 3b, 3c), or to provide a common identification procedure, through the medium of a network-related unit (5) or corresponding entity. Each such ID-certificate is accepted by a chosen number of network-connected actors (3a, 3b, 3c).

WO 02/21799 A1

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

NETWORK RELATED IDENTIFICATION SYSTEM

FIELD OF INVENTION

The present invention finds its application in networks or data networks, such as the Internet, and relates generally to a network-related user identification system.

The invention is based on a system in which a number of actors, at least two, and also a number of users connect to the network. The actors and the users are able to communicate with one another via the network.

More particularly, the present invention relates to a network-related user identification system in which one or more users can be initially identified via an established process chosen by the actor or some corresponding entity, and also allotted a secret code, this information being entered as a safe actor identification, said actor being referred to as a "first" actor hereinafter.

The invention has primarily been devised in respect of an application of the system in which the actors that can connect to the network consist of banks and in which the users that can connect to said network consist of bank customers.

The basic principles of the invention, however, can be generalised to such an extent as to enable said principles to be used also for other actors and for other users, as will be apparent from the various selected exemplifying objects evident from the following description.

DESCRIPTION OF THE BACKGROUND ART

Several network-related user identification systems of the aforedescribed kind are known to the art.

However, systems of the kind to which the invention relates and in which an actor shall be able to communicate with its users via a data network, such as the Internet, requires initial identification of each of these users before a chosen communication can be established.

Thus, each of a number of users will be identified positively and unequivocally by an actor, said actor being referred to as the "first" actor hereinafter.

Systems of the kind intended that utilise a data network or network and can be served by two or more actors with each actor being tied to users is normally based on each actor having developed its own procedure for enabling each of its users to be identified unequivocally.

Such an identification adapted procedure is normally based on the user presenting itself personally to the actor, providing or showing requested identification documents and being supplied by the actor with a unique term that applies solely between the actor and the user and that in respect of other actors and users constitutes a secret term, a PIN code or the like.

In the case of banks and credit institutions, a user will normally visit the bank personally, where a bank official will check the identity of the person concerned, through the medium of a driver's license, passport or some other official identification document that includes a photograph and a signature.

In this application, it has been found that each actor, such as a bank, has elected to create and utilise an own handshake procedure or routine for the identification of future contacts with the user, by giving respective users one or more unique terms that shall be exchanged between the user and the bank with each communication, so as to be able to establish the authority of the user safely and unequivocally.

SUMMARY OF THE PRESENT INVENTION

TECHNICAL PROBLEMS

When taking into consideration the technical deliberations that a person skilled in this particular art must make in order to provide a solution to one or more technical problems that he/she encounters, it will be seen that on the one hand it is necessary initially to realise the measures and/or the sequence of measures that must be undertaken to this end, and on the other hand to realise which means is/are required in solving one or more of these problems. On this basis, it will be evident that the technical problems listed below are highly relevant to the development of the present invention.

When considering the present state of the art as described above, it will be seen that in respect of a network-related user identification system that utilises a data network or network a technical problem resides in creating conditions whereby one or each user accepted by an actor can obtain a method of identification that is common to several actors and an ID-certificate adapted to this end.

Another technical problem is one of realising the significance of being accepted via a first actor through the medium of an established procedure chosen by the actor or the like and therewith be identified by the first actor, and also in the significance of creating conditions such that the first actor will be adapted to allocate individually to one or more user's identified solely by said first actor a procedure that is common to one or more second actors or to issue an ID-certificate, regardless of the identification and the handshake routines that said second actors have chosen for their users.

It will also be seen that a technical problem resides in the ability of substantially increasing the effectiveness of the actors so that said actors can utilise those databases with identified customers that the actors in the form of banks

have at their disposal - without needing to invest in and maintaining interfaces and program support for communication with each and every one.

Another technical problem resides in providing said actors with a standardised interface and connection agreement, where the actors can connect to an ID-certificate issuing bank via which agreement the actors will have disposal over identification data or information from all of the ID-certificates of the actors participating in the group.

It will also be seen that a technical problem resides in the creation of conditions whereby the actors or the banks in their turn need not co-ordinate a re-arrangement or alteration, a possible phase-out, modification, etc., of its existing ID routines, whereby all parties need solely to enter an agreement, a standard and procedure for a new ID service that can be based on the techniques originally established by each actor or bank - without these needing to be co-ordinated and utilise a substantial gain in effectivity in respect of both actors and users, such as banks and bank customers.

Another technical problem resides in realising the significance of and the advantages associated with creating such routines in said unit and utilising a rulebook in a manner such that each ID-certificate can be accepted by a chosen number of group co-ordinated actors connected to the network.

Another technical problem resides in realising the significance of and the advantages afforded by allowing said unit to be given the form and/or the function of an ID-exchange.

A technical problem also resides in realising the significance of and the advantages afforded by allowing said unit to include from one to all selected actors in a group-adapted rulebook, so that each of these actors can issue an ID-certificate or the like that is valid for all other actors co-ordinated in said group.

Another technical problem resides in realising the significance of incorporating in said unit an agreement complex based on principles that enable them to be executed via existing data standards.

Another technical problem resides in the ability to create with the aid of simple means conditions that allow said first actor to be adapted to inhibit a user-allocated ID-certificate stored in said unit in the event of a deficiency occurring in an established procedure in respect of a user.

Another technical problem is one of realising the significance of and the advantages afforded by also allowing an activated ID-certificate to be stored in a terminal allocated to a user, such as in a computer unit, mobile telephone or corresponding device, and therewith be useable directly in the activation of a selected transaction that requires an ID-certificate and secret data (PIN code) coupled to said certificate.

A further technical problem is one of realising the significance of and the advantages associated with allowing a system that can be based on a common safe identification of each item chosen by a unit that can be considered to belong to one or more current actors among a plurality of actors, via a network that is common to said user and said actors, and where the user shall be identified by at least by one of said actors via an established procedure.

Another technical problem resides in realising the significance of and the advantages associated with allowing a group of co-ordinated actors to co-act with a network-related unit or corresponding device such as to provide a method or corresponding procedure common to said group of co-ordinated actors for safe identification of different users via said network, and to allow at least one actor to function as a guarantor with respect to the identity of a selected user of said unit, and to allow said unit in response to such positive user identification to allocate to said user the possibility

of utilising said common method or procedure, by allocating to the user an ID-certificate together with associated secret terms.

In respect of a system in accordance with the invention, a technical problem also resides in creating conditions whereby each user can request access to a common method or procedure for identification or an ID-certificate from said first actor, where identification in accordance with said established procedure has already taken place, and in which said first actor can forward said request to said unit and where said guaranteed identity and/or ID-certificate of said user is stored.

Another technical problem is one of realising the significance of and the advantages associated with allowing said common method or procedure to include the use of a data structured ID-certificate and to enable any of said actors to identify a user of said unit via said ID-certificate upon receipt of such an ID-certificate from said user.

Another technical problem is one of realising the significance of and the advantages associated with allowing said ID-certificate to be adapted for a plurality of chosen, preferably different, applications.

Still another technical problem is one of realising the significance of and the advantages associated with allowing the issued ID-certificate to be received by and stored in a user-accessible terminal, and by enabling said user to use said issued ID-certificate upon each contact with any one of said group-associated actors when accessing said network via said terminal.

Another technical problem is one of realising the significance of allowing said ID-certificate to include asymmetrical key pairs and to store said ID-certificate in an encrypted form both in said terminal and in said unit.

It will also be seen that a technical problem resides in realising the significance of and the advantages associated with the use of a first computer program product that includes a computer program code which is adapted to allow those steps concerning communication of an actor with said unit and communication of an actor with said user when the program code is executed by a computer that is accessible to the actor, in accordance with the inventive system.

Another technical problem resides in the provision of a second computer program product that includes a computer program code which is adapted to carry out the steps concerning communication of a unit with an actor and the communication of said unit with a user when said code is executed by a computer that is accessible to said unit, in accordance with the inventive system, although with the exception of such communication that is included by said established and known initial identification procedure or routine.

Another technical problem resides in the provision of a third computer program product that includes a computer program code which is adapted to perform the steps that concern communication of a user with a unit and the communication of the user with an actor when said code is executed by a computer that is accessible to said user, in accordance with the inventive system, although with the exception of such communication that is included by said established and known initial identification procedure.

Still another technical problem is one of providing a carrier medium which carries a computer program code requisite for given computer program products.

Another technical problem is one of providing a data readable medium on/in which the computer program code used for the computer program product is stored.

SOLUTION

The present invention is thus based on a network-related user identification system where a number of actors, at least two actors, are connected to a data network or network, and where a plurality of users are also connected to said data network or network, and where the actors and the users are able to communicate with each other via said network and via established routines.

It is also necessary that one or more users are positively identified by one or more actors, such as at least one first actor, via an established procedure or routine chosen by an actor or corresponding entity.

With the intention of solving one or more of the aforesaid technical problems, it is proposed in accordance with the present invention that said first actor shall be adapted to allocate to one or more of the users identified by said first actor an ID-certificate that is valid for several actors or remaining actors via a network-related unit or corresponding device, and for said ID-certificate to be accepted by a chosen number of group co-ordinated, network-connected actors.

In accord with proposed embodiments that lie within the concept of the invention, it is proposed that said unit will include a rulebook that is adapted for all selected and group-orientated actors, so that each of said actors will be able to issue an ID-certificate that is valid in respect of and accepted by all remaining actors.

It is also proposed that the unit will beneficially be able to include an agreement complex that is based on principles which enable said agreement to be executed via existing data standards.

According to one embodiment, at least said first actor shall be adapted to permit the ID-certificate allocated to said

user to be inhibited in the unit in the event of a deficiency or non-agreement in an established user procedure or routine.

It is also proposed that the ID-certificate can be stored in a user-allocated terminal, such as a computer unit, mobile telephone or corresponding device.

The invention is thus based on a system which provides positive (secure) identification of each selected user of a number of actors via a network which is common to said user and said actors, via an established procedure or routine, and that said user shall be identified by at least one first actor among said group-associated actors.

It is proposed in accordance with the invention in this respect that the actors shall co-act with a network-related unit or corresponding function to provide a method of user identification that is common to said actors via said network, that said user can be identified by said first actor via said established procedure or routine, that said first actor can guarantee the identity of the user of said unit through the medium of said established procedure, and that said unit assigns to said user the possibility of using this common procedure or an ID-certificate in response to such user identification.

It is also proposed that a user shall be able to request access to a common identification procedure from said first actor where identification according to said established procedure has already been carried out, and that the first actor is able to forward the request to said unit with a guaranteed identity of the user.

It is also proposed that this common procedure will beneficially include the use of a data structured ID-certificate, and that any one of said group-associated actors shall be able to identify the user of said unit via said ID-certificate upon receipt of such an ID-certificate from a user.

It is also proposed that one and the same ID-certificate can be used for a number of different applications.

It is also proposed that the ID-certificate can be received by and stored in a user allocated terminal, such as a computer unit, mobile telephone or corresponding device, and that the user is able to use said ID-certificate to establish contact with one or each of said group-associated actors upon access to the network via said terminal.

In addition, it is proposed in accordance with the invention that the ID-certificate can be allowed to contain asymmetric key pairs, and that the ID-certificate can be stored encrypted in both said terminal and said unit.

It is also proposed that one or more of said actors is comprised of: a loan institution, such as a bank, a supplier of goods and/or services, such as a shop or an insurance company, one or more authorities, such as taxation authorities or an unemployment benefit society.

The invention also relates to the use of a first computer program product, a second computer program product, a third computer program product, a data carrying medium, and to a computer readable medium to this end.

ADVANTAGES

Those advantages primarily characteristic of a network-related user identification system that includes a network which functions as a data network, and actors and users that can connect to said network in accordance with the present invention reside in the provision of conditions that allows a first actor who is responsible for a correct and positive identification of each user associated with said actor to be adapted and trusted to allocate to one or more users identified by said first actor with ID-certificates that are valid to one or more other actors associated in a group of actors, via a network-related unit or corresponding device, and in

that each such ID-certificate will be accepted by a chosen number of group-related and network-connected actors.

In addition, it is believed that the invention will substantially increase the efficiency of the actors, which will be able to utilise those databases with identified customers that the actors, in the form of banks, have at their disposal, without needing to invest in and maintain interfaces and program supports for communication with each and every one.

The actors are offered a standardised interface and connection agreement where the actors can connect to a bank issuing an ID-certificate, said actors being able to have at their disposal identification information contained in all of the ID-certificates of actors participating in said group, via the aforesaid agreement.

In turn, neither the actors nor the banks need co-ordinate alterations, modifications and possible phase-outs, etc., of their existing ID routines.

All parties need only subscribe to an agreement, a chosen standard and a defined procedure for a new ID service that can be based on those techniques that have been originally established by an actor or a bank - without these entities needing to be co-ordinated. This results in a considerable efficiency gain with respect to both actors and users, such as banks and bank customers.

The primary characteristic features of a network-related user identification system having features significant of the present invention are set forth in the characterising clause of the accompanying Claim 1.

BRIEF DESCRIPTION OF THE DRAWINGS

A network-related user-identification system at present preferred and having features significant of the present invention will now be described in more detail by way of example with reference to a number of applications and also with reference to the accompanying drawings, in which

Figure 1 is a highly simplified illustration of a first embodiment of an inventive user identification system;

Figure 2 illustrates a switching sequence in which the order and the delivery of an ID-certificate can be effected via the "standard Internet bank" of a user;

Figure 3 illustrates a first example of the application of the system in which an authority wishes to broadcast information with the aid of an ID-exchange and a user-associated ID-certificate;

Figure 4 illustrates another example of the application of the system in which a bank service shall be offered with the aid of an ID-exchange and a user-associated ID-certificate;

Figure 5 illustrates a third example of the application of the system in which payment shall be made to an Internet shop with the aid of an ID-exchange and a user-associated ID-certificate;

Figure 6 illustrates a fourth example of the application of the system in which a payment transaction shall be carried out with the aid of an ID-exchange and a user-associated ID-certificate;

Figure 7 illustrates an application in which identification can be ordered from a certified company connected to an ID-exchange;

Figure 8 illustrates a fifth example of the application of the system in which a user intends to send documents of a confidential nature to an authority, through the medium of an ID-exchange and a user-associated ID-certificate; and

Figure 9 is a block diagram illustrating a number of functions significant to an ID-exchange.

DESCRIPTION OF EMBODIMENTS AT PRESENT PREFERRED

Figure 1 thus illustrates a network-related user identification system 1 in which at least two actors 3, 3a (3b, 3c) and a plurality of users are connected to the network 2, in the illustrated case the Internet. Of the aforementioned plurality of users, solely the user 4 associated with the actor 3 and the user 4a associated with the actor 3e have been shown in the Figure.

Figure 1 is intended to illustrate that the user 4a could be an authority (see Figure 3) or an individual corresponding to the person 4.

The person or user 4 has access to a terminal 4a', which is a computer unit in the case illustrated.

Each such terminal 4a' shall have a capacity and a function which enables it to perform requisite storage under secure forms. This applies in particular to the storage of an ID-certificate, as described in more detail hereinafter.

In dialogue with the actor 3, the terminal 4a' shall be able to confirm its own authority and the authority of the actor 3, by acknowledging a secret term or secret code.

Confirmation of the authority of a person 4, etc., is normally based on a code that is valid between the person 4 and

the actor 3 and that is secret to other actors and users, referred to as a "secret" code or term.

Although this normally concerns a PIN code, it may also concern some other secure person-related unique method for use when issuing an identity or when demanding an identity.

The actors 3, 3a and the users 4, 4a can communicate with each other via the network 2 in a known manner, and consequently the measures and means required for such communication will not be described in detail in this document.

One or more users is/are identified in a known manner in a first actor 3 via a procedure or routine 30 established by an actor, such as said first actor 3 or some corresponding entity, only one user 4 being shown to the left in the Figure for sake of clarity.

This identification is referenced 4' and is stored by the actor 3.

The user 4 is considered to be a bank customer in the following description, while the actor 3 is considered to be a bank.

The first actor or the bank 3 chooses the procedure 30 by which the user or the bank customer 4 shall identify himself/herself and which identification data 4' shall be stored by the first actor 3.

This procedure 30 is based on the user 4 personally identifying himself/herself to a bank official and providing a photograph, signature and other information required to confirm the person's identity.

The bank 3 now chooses to create its own handshake routines 30', so that the user 4 can thereafter identify himself/herself to the first actor 3 in a well structured and secure manner.

In addition to this actual identification, the identification procedure 4' normally includes the provision of one or more secret terms, such as a PIN code.

The system 1 also includes at least one further actor, referenced 3a, which permits a user 4a to identify himself/herself, via an own procedure 30a and an own handshake routine 30a'. The user 4a may also be a bank customer in this case and has been illustrated as an authority or an administration.

Reference signs 3b and 3c are intended to show that more actors than those referenced 3 and 3a can be connected to the data network or the network 2.

According to the invention, one of the actors, such as said first actor 3, shall be adapted to allocate to one or more users, such as the user 4, an ID-certificate (4) which is valid in respect of one or more actors, such as the actor 3a, among a plurality of second available and group-associated actors, or a common procedure for identifying that each such ID-certificate (4) shall be accepted by a chosen number of network-connected actors, such as the actors 3a (3b, 3c) in addition to their own identifications 4', this being effected through the medium of a network-related unit 5 or some corresponding device, either virtual or real.

The unit 5 may, of course, consist of a register of issued ID-certificates, where said unit 5 can be read by each of the actors 3, 3a and where access to said unit 5 is fully independent of the choice of their handshake routines.

The unit 5 need not be a physical unit and nor yet one or more physical units.

The unit 5 shall beneficially be considered as being a virtual unit whose functional responsibility and operative par-

ticipation is controlled by a rule mechanism adapted for all group-related actors 3, 3a.

Thus, an actor 3 can place in the unit 5 either an original notation of issued ID-certificates (4) or a copy thereof.

The unit 5 may also include the address data, rules, etc., required in order to answer questions that are asked with respect to the validity of the ID-certificate concerned.

The unit 5 is, of course, complex with respect to its construction and structure, but can be considered functionally as an ID-exchange in which a plurality of ID-certificates, such as ID-certificate (4) allocated to selected users upon request can be stored, and includes a rulebook adapted for all selected actors 3, 3a, 3b, 3c so that each of said actors can issue an ID-certificate that is valid for all or remaining group-associated actors.

The unit 5 may also include an agreement complex based on principles that enable it to be executed via existing data standards.

Certain selected functions of the unit are shown in the block diagram of Figure 9.

The first actor 3 (and also other actors) is (are) adapted to inhibit a user-allocated ID-certificate (4) entered into and stored in the unit 5, when noting a deficiency in an established procedure 30, 30' concerning its own actor-associated user, such as the user 4.

The ID-certificate (4) may also be storable in the terminal 4a' of a user 4, such as a data unit or computer unit.

In summary, Figure 1 can be considered to show that the user 4 has at its disposal a soft ID-certificate (4) that is stored in the terminal 4a' of the user or bank customer 4.

The ID-certificate (4) is allocated to the ID-exchange 5, said ID-exchange consisting of a bank-common ID-exchange that issues, handles and checks all user-associated ID-certificates (4) on behalf of the banks.

The banks 3, 3a (3b, 3c) have a mutual agreement whereby each bank accepts the procedure 30, 30' and handshake routines of the other bank or banks such as to provide secure services to their customers 4, and each bank 3 is able to issue an ID-certificate that is valid in respect of all group-associated banks 3a (3b, 3c) on the basis of these procedures and routines.

Figure 2 shows that a request for and the delivery of an ID-certificate (4) can be effected via the standard Internet bank of the user or customer.

In this regard, the user or bank customer 4 connects to his/her Internet bank, logs on with his/her normal security code and chooses to collect his/her ID-certificate (4).

The bank 3 now checks the identity of the customer and provides the customer with a "ticket" for secure linking to the ID-exchange 5.

The ID-exchange 5 now delivers the ID-certificate (4), which can be stored encrypted on the hard disk of the user's terminal 4a'.

Figure 3 shows a first example of the application of the system wherein an authority 7 wishes to spread selected information with the aid of the ID-exchange 5 and a user-associated and personal ID-certificate (4).

The illustrated procedure comprises the steps whereby an authority 7 sends an e-mail message announcing that stored information is found for collection. The user 4 then connects to the authority 7 and identifies himself with the aid of his ID-certificate (4).

The authority 7 then sends a certificate transaction and an ID-certificate (4). This transaction requires a validity check and a plurality of protocols are available to this end.

In the illustrated example, there is used a validity check that includes a known standard, designated "OCSP", which is an acronym for OnLine; Certificate; Status and Protocol.

The ID-exchange 5 checks that the ID-certificate (4) is valid and sends a message to this effect back to the authority 7.

The receiver 4 can now read the information, sent via an encrypted transmission. The authority 7 will then be aware that the user or the customer 4 has collected the requisite information.

Figure 4 shows another example of the application of the system wherein bank services are offered through the medium of an ID-exchange 5 and can be released with the aid of a personal ID-certificate (4).

When using this service in the bank 3a, the ID-certificate (4) is used in the communication with the Internet bank from the user 4.

The Internet bank 3a sends a certificate transaction to the ID-exchange 5.

The ID-exchange 5 checks that the ID-certificate (4) is valid and sends a message to this effect back to the Internet bank 3a.

The user 4 is then able to carry out the errand in the Internet bank 3a securely.

Figure 5 illustrates a third example of the application of the system wherein payment is made with the aid of an ID-exchange 5.

When making payment to an Internet shop 8, an ID-certificate (4) and the bank giro address of the user are sent to the Internet shop 8.

The Internet shop 8 sends to the ID-exchange 5 a certificate transaction including the amount to be paid and the bank giro address of the user.

Figure 6 shows a fourth example of the application of the system wherein a payment transaction is effected with the aid of an ID-exchange 5 and a personal ID-certificate (4).

In this application of the system, the ID-exchange 5 checks the validity of the ID-certificate (4) and sends the amount concerned and the bank giro addresses of the receiver and the sender to a bank giro central agency 9.

The bank giro central agency 9 translates bank giro addresses to account numbers, checks for sufficiency of funds in the purchaser's account and transfers the purchasing sum to the account of the Internet shop in a bank 3a.

The ID-exchange 5 informs the Internet shop 8 that the purchasing sum has been paid into the account and that delivery can now take place.

Figure 7 shows that an identification can also be quoted from a certified company 10 connected to the ID-exchange 5.

In this case, a bank customer 4 connects to an Internet bank 3 or an authority connected to the ID-exchange and is linked through said bank or authority with the ID-exchange 5.

The bank customer 4 is given an encrypted input field through which the customer can identify itself to its standard Internet bank 3.

The ID-exchange 5 now links the ID-query to the bank 3, which checks the identity of the customer 4 and provides (sends) the customer with a "ticket" for secure linking to the ID-exchange 5.

The ID-exchange 5 delivers the ID-certificate (4), which is stored encrypted on the hard disk of the customer 4 in the terminal or computer unit 4a'.

Figure 8 shows a fifth example of the application of the system in which the user 4 or customer seeks contact with an authority 7 through the medium of the ID-exchange 5 while using a personal ID-certificate (4) with the intention of depositing electronically applications, statements, income tax returns, etc.

The user or customer 4 now sends information to the authority 7 authenticated with the aid of his/her private key and encrypted with the public key of the authority, knowing that only the authority 7 can read the transmitted information.

The information may have the form of statements, income tax returns, applications for student loans, applications for housing allowances, changes in securities (stocks, bonds, shares) with the authority concerned, etc.

The authority 7 is now able to receive the information sent by the user 4.

The authority now asks the ID-exchange 5 whether the receiver's ID-certificate (4) is valid or not.

The ID-exchange 5 checks the validity of the ID-certificate (4) and sends the answer back to the authority 7 via a transaction.

Although system application can be made more comprehensive and more sophisticated than has been described above with reference to the exemplifying applications, it will neverthe-

less be seen that the system 1 is adapted to afford positive identification of a chosen user 4 of a number of different actors 3, 3a, via a network 2 which is common to said user and said actors, where the user 4 is identified 4' by the first of said actors 3 via an established procedure.

The actors 3, 3a (3b, 3c) thus co-operate with one and the same network-related unit 5 such as to provide for said actors a common procedure that enables positive (safe) identification of different users 4 via the network 2.

The user 4 can thus be identified by said first actor 3 via the aforesaid established procedure 30, and the first actor 3 is able to guarantee the identity of the user (4) in respect of said unit 5, and in response to this identification of said user 4 the unit is able to provide the user with the possibility of using said common procedure for other actors.

The aforedescribed examples illustrate that a user 4 is able to request access to a common method for identification or an ID-certificate (4) from said first actor, where identification 4' has taken place in accordance with the established procedure 30 and said first actor 3 is able to forward the request to said unit 5 together with said guaranteed identity and said user ID-certificate (4).

When the user 4 requests access to said common procedure for identification from a second actor 3a, said second actor 3a forwards the request to the network-related unit 5, wherewith said unit forwards said request to the first actor 3 where said identification 4' according to said established procedure 30 has taken place, and said first actor 3 forwards said request to said unit 5 with said guaranteed identity (4) of the user 4.

In this case, the common procedure includes the use of a data-structured ID-certificate (4) and enables any one of the aforesaid actors to identify the user 4 of said unit 5 via

said ID-certificate, upon receipt of such an ID-certificate (4) from a user 4.

It lies within the scope of the present invention to use the ID-certificate (4) for a number of different applications, such as authentication, signing, encryption and/or alteration protection.

The ID-certificate (4) shall, in particular, be received by and stored on a user-accessible terminal, such as a computer unit 4a', and the user is able to use said ID-certificate (4) when in contact with one of said actors, subsequent to accessing the network 2 via the computer unit 4a'.

It is particularly suitable to include asymmetric key pairs in the ID-certificate (4), and to store the ID-certificate (4) encrypted in said terminal, such as the computer unit 4a' and in said unit 5.

It lies within the scope of the invention for the terminal 4a' to comprise a portable unit, such as a portable computer or a mobile telephone, or to comprise a more stationary unit, such as a personal computer.

The terminal 4a' may also comprise a card-associated unit, such as a computer unit that co-acts with a smart card that can be read by a card reader provided for this purpose.

It also lies within the scope of the invention to assign a limited validity time to the ID-certificate (4).

There is nothing to prevent the ID-certificate (4) from being renewed subsequent to acceptance by the first actor 3.

When necessary, any one of said actors 3, 3a (3b, 3c) is able to lockout or block the ID-certificate (4) in said unit 5 when an attempt to force (break) or misuse the ID-certificate (4) is detected.

One or more of said actors may comprise a loan institution, such as a bank, a goods intermediary and/or a service intermediary, such as a shop or an insurance company, an authority, such as an inland revenue authority or an unemployment benefit society.

The present invention can be used to particular benefit on a data network or network consisting of the global network "Internet".

The invention also relates to a first computer program product which includes a computer program code which, when executed by a computer that is accessible to an actor 3, is able to perform the steps concerning communication of the actor 3 with a unit 5 and also the steps concerning communication of the actor 3 with a user 4 in accordance with the aforedescribed system and its mode of application.

The invention also relates to a second computer program product that includes a computer product code which, when executed by a computer that is available to a unit 5, is able to perform the steps that concern communication of the unit 5 with an actor 3 and also communication of said unit 5 with a unit 4, in accordance with the aforedescribed system and its applications, although with the exception of such communications as those that are included by said established procedure and that are thus previously known.

The invention also relates to a third computer program product that includes a computer program code which, when executed by a terminal or a computer unit 4a' accessible to a user 4, is able to perform those steps that concern communication of said user 4 with a unit 5 and also concern communication of the user 4 with an actor 3 in accordance with the aforedescribed system application and also with further applications, although with the exception of such communication as that which is included by said established procedure 30 and is thus previously known.

The invention also relates to a data carrying medium that is adapted to carry a computer program code required in accordance with the aforesaid first, second and third computer program products.

The invention also relates to a computer readable medium that utilises a computer program code according to the first, the second or the third computer program product and stored on said medium.

The network-related unit or the ID-exchange 5 shall be capable of utilising a number of functions, of which those listed below have particular significance.

A first function 5a is adapted for verification of a link from a bank;
- a second function 5b is adapted to create and allocate an ID-certificate;
- a third function 5c is adapted to supply information to a bank;
- a fourth function 5d is adapted to receive/handle any lock-outs or blocks;
- a fifth function 5e is adapted to receive/handle queries relating to security checks and used standards (OCSP);
- a sixth function 5f is adapted to deliver security-checked replies;
- a seventh function 5g is adapted to permit connection to a new bank;
- an eighth function 5h is adapted to allow a company/authority to connect to a given bank;
- a ninth function 5i is adapted to provide statistics and evaluate traceability;
- a tenth function 5j is adapted to set the fee for the identity confirmation services between co-ordinated banks; and
- an eleventh function or service 5k is adapted to "clear" fees between co-ordinated banks.

It can be mentioned in summary that banks involved in the system can play three different roles, these being

- as an enquiry bank on behalf of an end customer in respect of the identity given by the customer;
- as an answering bank based on customers identified in its own customer databases in reply to queries via the ID-exchange 5;
and
- as a selling bank of own identities and the identities of other participating banks with respect to questioned customers via a security application that purchasing companies/authorities can be linked to the ID-exchange in accordance with said agreement when customers visit the home page concerned.

With respect to the asymmetric keys, there can be used the "system PKI" (Public Key Infrastructure), with which a "key encryption and secret code" strategy is carried out.

It will be understood that the invention is not restricted to the aforedescribed illustrative examples thereof and that modifications can be made within the scope of the inventive concept as illustrated in the following Claims.

CLAIMS

1. A network-related user identification system wherein a number of actors, at least two, are connected to the network, wherein a plurality of users are connected to said network, wherein the actors and the users can communicate mutually via said network, and wherein one or more users is/are identified by at least one actor, a first actor, via a chosen procedure established by the actor or a corresponding entity, **characterised** in that said first actor is adapted to allocate to one or more users identified by said first actor an ID-certificate that is valid in respect of several actors for a common identification establishing procedure, via a network-related unit for corresponding elements; and in that each such ID-certificate is accepted by a chosen number of network-connected actors.

2. A system according to Claim 1, **characterised** in that said unit has been given the form of an ID-exchange.

3. A system according to Claim 1 or 2, **characterised** in that said unit includes a rulebook adapted for all chosen actors such that each of said actors can issue an ID-certificate that is valid with respect to all co-ordinated actors.

4. A system according to Claim 1, 2 or 3, **characterised** in that said unit includes an agreement complex based on existing data standards.

5. A system according to Claim 1, **characterised** in that at least said first actor is adapted to inhibit a user-assigned ID-certificate in the unit among other things when a deficiency is detected in an established user procedure.

6. A system according to Claim 1, **characterised** in that said ID-certificate can be stored in the terminal of a user, such as a computer unit.

7. A system for providing positive identification of a chosen user by a plurality of different actors via a network that is common to the user and to the actors, wherein said user is identified by a first actor among said actors via an established procedure, **characterised** in that said actors co-operate with a network-related unit for providing a user identification procedure that is common to said actors, via said network; in that said user can be identified by said first actor through the medium of said established procedure; in that said first actor can guarantee the identity of the user of said unit through the medium of said established procedure; and in that said unit provides the user with the possibility of using said common procedure upon identification of said user.

8. A system according to Claim 1 or Claim 7, **characterised** in that a user is able to request from said first actor access to a common identification procedure, where identification according to said established procedure has already been carried out by said first actor; and in that said first actor forwards the request to said unit together with said guaranteed identity of the user.

9. A system according to Claim 1 or Claim 7, **characterised** in that a number of banks having mutually the same or mutually different identification routines are co-ordinated to accept one and the same ID-certificate.

10. A system according to Claim 1, 7, 8 or 9, **characterised** in that said common procedure includes the use of an ID-certificate; and in that any one of said actors can identify a user of said unit via an ID-certificate, upon receipt of said ID-certificate from said user.

11. A system according to Claim 10, **characterised** in that said ID-certificate can be used in respect of a number of

different applications, such as authentication, signing, encryption and/or alteration protection.

12. A system according to any one of the preceding Claims, **characterised** in that the ID-certificate is received by and stored on a user-accessible terminal, such as a computer unit; and in that said unit is able to use said ID-certificate upon contact with any one of said actors, subsequent to accessing the network via said computer unit.

13. A system according to Claim 12, **characterised** in that said ID-certificate includes asymmetric key pairs; and in that said ID-certificate is stored encrypted in both the computer unit and in said unit.

14. A system according to Claim 12 or 13, **characterised** in that said terminal is a portable unit, such as a portable computer unit or a mobile telephone.

15. A system according to Claim 12 or 13, **characterised** in that said terminal is a stationary unit, such as a personal computer.

16. A system according to Claim 12 or 13, **characterised** in that said terminal is a card-associated unit, such as a computer unit that co-acts with a smart card that can be read by a card reader intended for this purpose.

17. A system according to any one of the preceding Claims, **characterised** in that said ID-certificate has limited validity.

18. A system according to Claim 17, **characterised** in that said ID-certificate can be renewed subsequent to acceptance by said first actor.

19. A system according to any one of the preceding Claims, **characterised** in that any one of said actors can lockout or block said ID-certificate in said unit when an attempt to is made to force said ID-certificate or said ID-certificate is misused.

20. A system according to any one of the preceding Claims, **characterised** in that one or more of said actors is a loan institution, such as a bank.

21. A system according to any one of the preceding Claims, **characterised** in that one or more of said actors is/are an intermediary of goods and/or services, such as a shop or an insurance company.

22. A system according to any one of the preceding Claims, **characterised** in that one or more of said actors is/are an authority, such as a taxation authority or an unemployment funding society.

23. A system according to any one of the preceding Claims, **characterised** in that said network is the global network "Internet".

24. A first computer program product, **characterised** in that the product includes a computer program code which, when executed by a computer that is accessible to an actor, is able to carry out the steps concerning communication of said actor with a unit and the steps concerning communication of said actor with a user, in accordance with the system defined in any one of the preceding Claims.

25. A second computer program product, **characterised** in that the second product includes a computer program code which, when executed by a computer that is accessible to a unit, is able to carry out the steps concerning communication of said unit with an actor and the steps concerning communi-

cation of said unit with a user, in accordance with the system defined in any one of Claims 1 to 23, with the exception of such combination as that which is included by said established procedure.

26. A third computer program product, **characterised** in that the product includes a computer program code which, when executed by a computer that is accessible to a user, is able to carry out the steps that concern communication of said user with a unit and also the steps that concern communication of said unit with an actor, in accordance with the system defined in any one of Claims 1 to 23, with the exception of such communication as that included by said established procedure.

27. A carrying medium, **characterised** in that said medium carries a computer program code required in accordance with one or more of Claims 24 to 26.

28. A computer readable medium, **characterised** in that the computer program code according to one or more of Claims 24 to 26 is stored on said medium.

Fig. 1

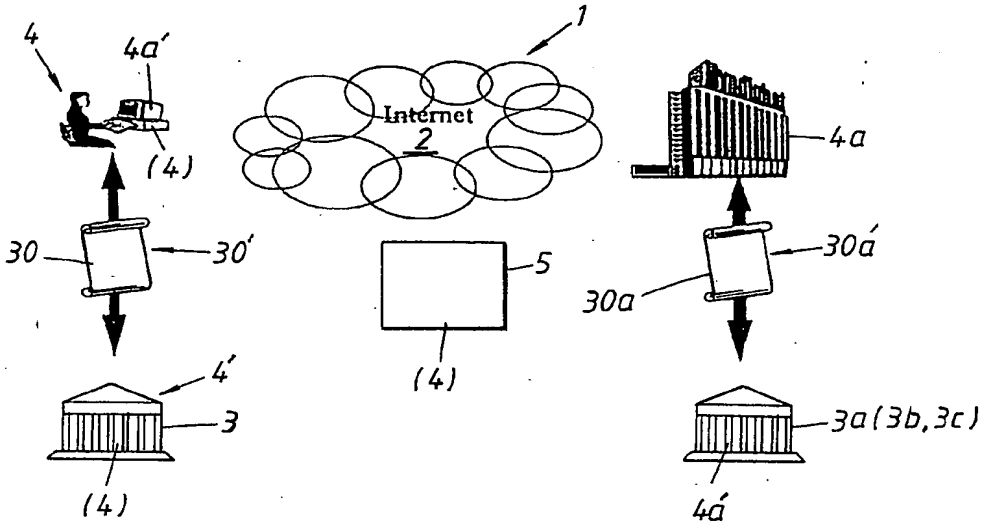

4
4a'
(4)
1
Internet
2
4a
30
30'
5
30a
30á
4'
3
(4)
3a (3b, 3c)
4á

Fig. 2

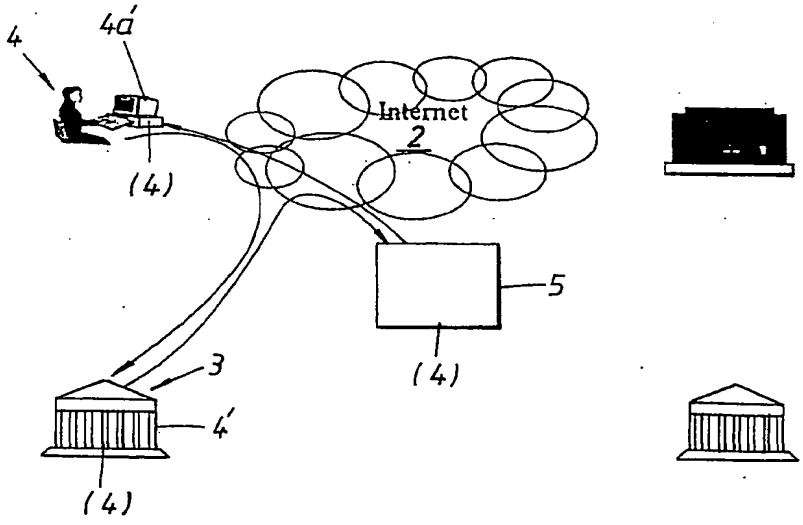

4
4á
Internet
2
(4)
5
3
4'
(4)

Fig. 3

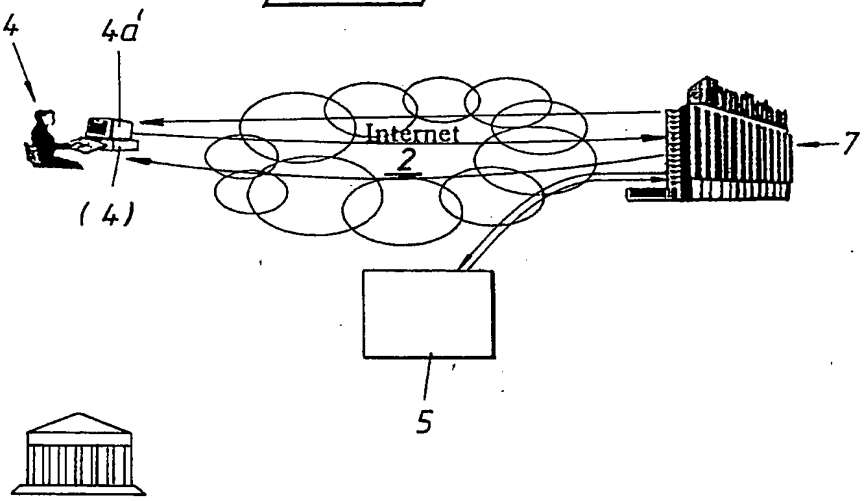


Fig. 4

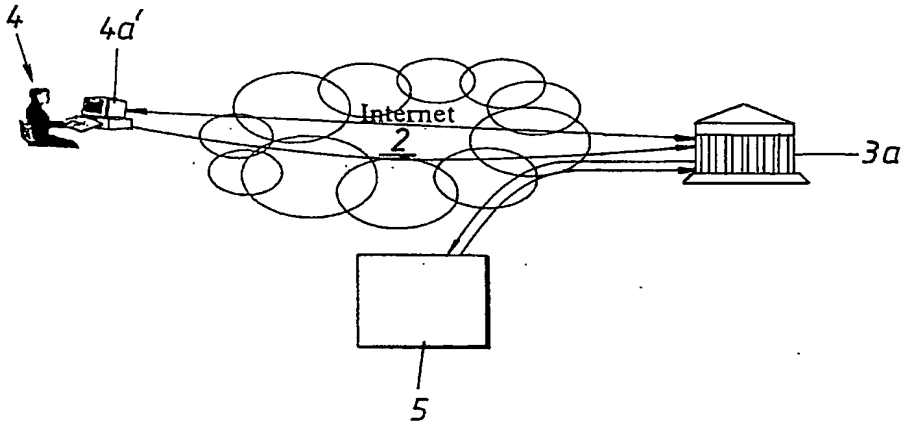


Fig. 5

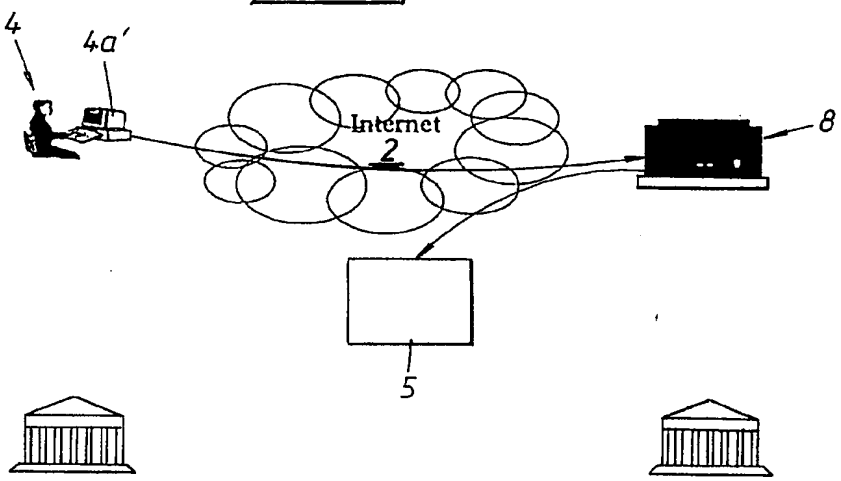


Fig. 6

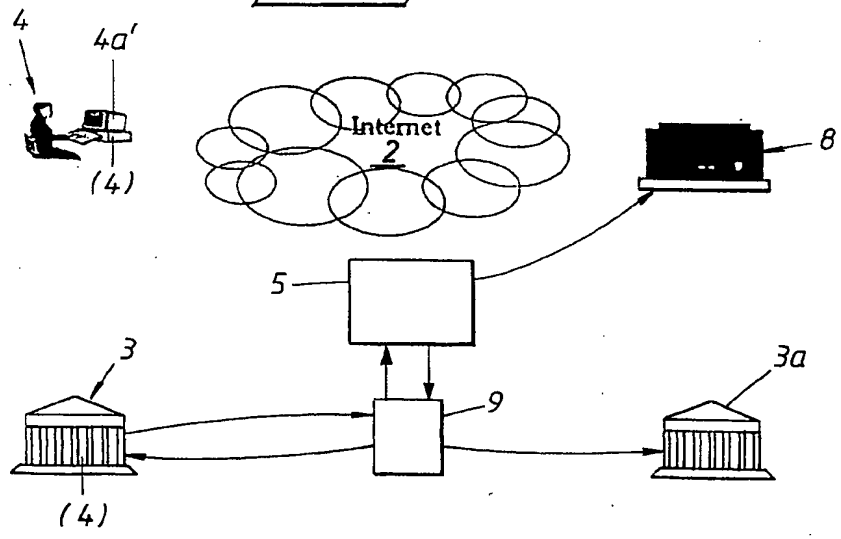


Fig. 7

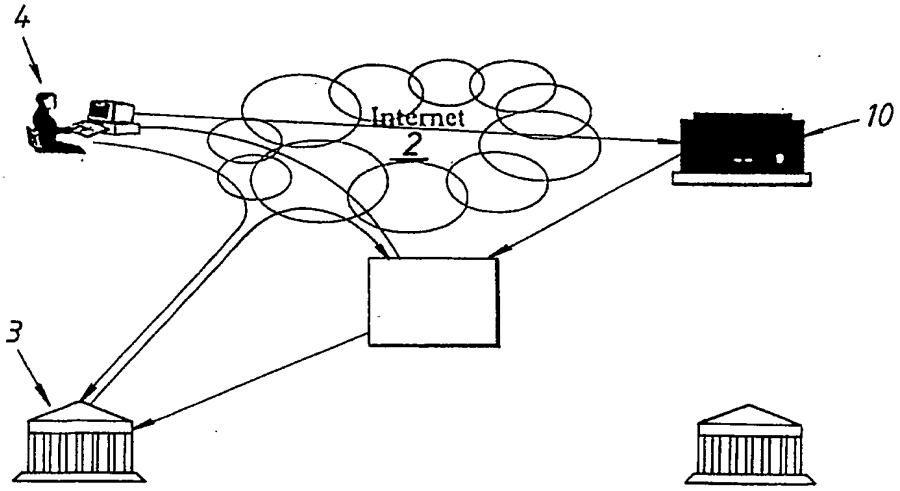


Fig. 8

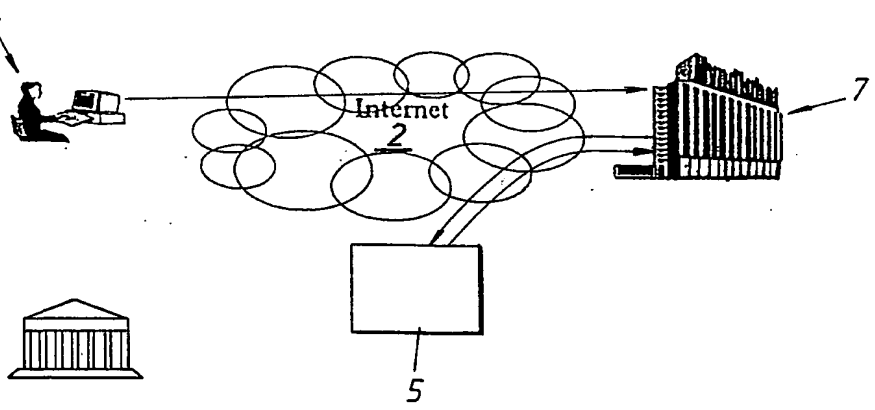
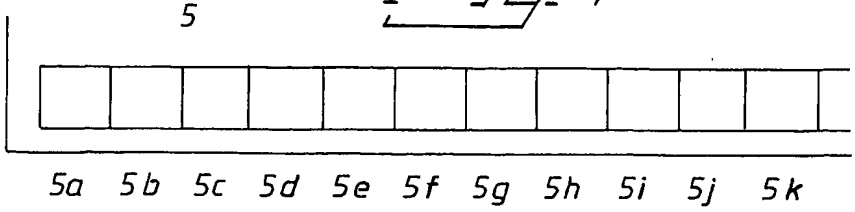


Fig. 9



INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01901

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 29/06, G06F 17/00, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 0048360 A1 (HICKS, MARCK ET AL.), 17 August 2000 (17.08.00), page 1, line 19 - page 6, line 13, abstract --	1-28
X	US 5745574 A (MUFTIC, SEAD), 28 April 1998 (28.04.98), column 4, line 54 - column 8, line 14, figures 1A-1B, abstract --	1-28
X	US 5903882 A (ASAY, ALAN ET AL.), 11 May 1999 (11.05.99), column 4, line 20 - column 9, line 9, figure 3, claim 1, abstract --	1-28

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 December 2001	04 -12- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Pär Heimdal/LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01901

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5659616 A (SUDIA, FRANK W.), 19 August 1997 (19.08.97), column 4, line 66 - column 5, line 15, claims 1-5, abstract --	1-28
A	EP 0942568 A2 (UNWIRED PLANET, INC.), 15 Sept 1999 (15.09.99), abstract, the whole document --	1-28
P,X	EP 1054545 A2 (AT&T CORP), 22 November 2000 (22.11.00), claim 1, abstract --	1-28
P,X	US 6285991 A (POWAR, WILLIAM L.), 4 Sept 2001 (04.09.01), column 4, line 31 - column 5, line 37, figures 1-5, abstract -- --------	1-28

INTERNATIONAL SEARCH REPORT

Information on patent family members

06/11/01

International application No.
PCT/SE 01/01901

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0048360 A1	17/08/00	AU 2878700 A	29/08/00
		AU 2878800 A	29/08/00
		WO 0048108 A	17/08/00
US 5745574 A	28/04/98	EP 1068697 A	17/01/01
		WO 9952242 A	14/10/99
US 5903882 A	11/05/99	AU 5515398 A	03/07/98
		BR 9714400 A	18/04/00
		CN 1244936 A	16/02/00
		EP 0965111 A	22/12/99
		JP 2001507145 T	29/05/01
		US 2001011255 A	02/08/01
		WO 9826385 A	18/06/98
US 5659616 A	19/08/97	AU 698454 B	29/10/98
		AU 3715695 A	16/02/96
		CA 2194475 A	01/02/96
		CZ 9700115 A	17/09/97
		EP 0771499 A	07/05/97
		JP 10504150 T	14/04/98
		NO 970084 A	10/03/97
		RU 2144269 C	10/01/00
		TR 970079 A	00/00/00
		WO 9602993 A	01/02/96
EP 0942568 A2	15/09/99	CN 1235448 A	17/11/99
		JP 11317735 A	16/11/99
		US 6233577 B	15/05/01
EP 1054545 A2	22/11/00	BR 0002291 A	06/02/01
US 6285991 A	04/09/01	AU 5382098 A	03/07/98
		EP 0961999 A	08/12/99
		WO 9826386 A	18/06/98